

#5

UNITED STATES PATENT AND TRADEMARK OFFICE



Applicants : Futoshi Hachimura
Serial No. : 09/990,001
For : COMMUNICATION SYSTEM, ITS CONTROL METHOD,
PROGRAM AND MEDIUM
Filed : November 21, 2001
Examiner : Unassigned
Art Unit : 2131

COPY OF PAPERS
ORIGINALLY FILED

Assistant Commissioner of Patents
Washington, D.C. 20231

CLAIM TO BENEFIT OF 35 U.S.C. § 119
AND FILING OF PRIORITY DOCUMENT

Claim is made herein to the benefit of 35 U.S.C. § 119 for the filing date of the following Japanese Patent Application No.: 2000-361285 (filed November 28, 2000).
A certified copy of this document is enclosed.

Dated: January 25, 2002

Respectfully submitted,

Marylee Jenkins
Reg. No. 37,645
An Attorney of Record

ROBIN, BLECKER & DALEY
330 Madison Avenue
New York, New York 10017
(212) 682-9640

RECEIVED

MAR 13 2002

Technology Center 2100

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to:
Assistant Commissioner for Patents, Washington, D.C. 20231, on:

MARYLEE JENKINS

Signature



日本特許庁
JAPAN PATENT OFFICE

168 US / fu

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office

出願年月日

Date of Application:

2000年11月28日

出願番号

Application Number:

特願2000-361285

出願人

Applicant(s):

キヤノン株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

COPY OF PAPERS
ORIGINALLY FILED

RECEIVED

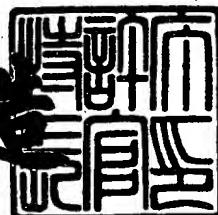
MAR 13 2002

Technology Center 2100

2001年12月21日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造



出証番号 出証特2001-3110569

【書類名】 特許願
【整理番号】 4176058
【提出日】 平成12年11月28日
【あて先】 特許庁長官殿
【国際特許分類】 H04L 9/00
【発明の名称】 通信システム及びその制御方法、及び媒体
【請求項の数】 24
【発明者】
【住所又は居所】 東京都大田区下丸子3丁目30番2号 キヤノン株式会社内
【氏名】 八村 太史
【特許出願人】
【識別番号】 000001007
【氏名又は名称】 キヤノン株式会社
【代表者】 御手洗 富士夫
【代理人】
【識別番号】 100081880
【弁理士】
【氏名又は名称】 渡部 敏彦
【電話番号】 03(3580)8464
【手数料の表示】
【予納台帳番号】 007065
【納付金額】 21,000円
【提出物件の目録】
【物件名】 明細書 1
【物件名】 図面 1
【物件名】 要約書 1
【包括委任状番号】 9703713
【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 通信システム及びその制御方法、及び媒体

【特許請求の範囲】

【請求項1】 情報端末に対して公開鍵暗号方式でWeb (World Wide Web) 電子メールサービスを行うサーバを有する通信システムにおいて、

前記サーバは、前記公開鍵暗号方式における秘密鍵を管理する管理手段を有することを特徴とする通信システム。

【請求項2】 前記管理手段は、前記秘密鍵の使用許諾を認証するための画面データを前記情報端末に供給する供給手段を含むことを特徴とする請求項1記載の通信システム。

【請求項3】 前記管理手段は、前記供給手段により供給された前記秘密鍵の使用許諾を認証するための画面データにおいて、該秘密鍵を暗号化する際に用いられたパスフレーズが前記情報端末から入力されることを条件として該秘密鍵の使用許諾を認証する認証手段を含むことを特徴とする請求項1又は2記載の通信システム。

【請求項4】 前記認証手段は、前記情報端末とサーバとの間において連続的に確立されている暗号通信を単位として前記秘密鍵の使用許諾を認証することを特徴とする請求項3記載の通信システム。

【請求項5】 前記認証手段は、前記情報端末とサーバとの間に一旦確立された暗号通信が異常終了し、その後同一の情報端末との間に暗号通信が確立された場合は、該異常終了に係る暗号通信に対して認証したままの秘密鍵の使用許諾を停止する操作を行うように該情報端末に指示することを特徴とする請求項3又は4記載の通信システム。

【請求項6】 前記認証手段は、前記情報端末とサーバとの間に暗号通信が確立されて前記秘密鍵の使用許諾を認証した後、一定時間経過することにより認証に係る秘密鍵の使用許諾を取消すことを特徴とする請求項3～5の何れかに記載の通信システム。

【請求項7】 前記サーバは、前記認証手段により使用許諾が認証された秘

密鍵に基づいて、前記情報端末から復号処理を要求された暗号化に係るWeb電子メールを復号して、該情報端末に送信する復号手段を有することを特徴とする請求項1～6の何れかに記載の通信システム。

【請求項8】 前記サーバは、前記認証手段により使用許諾が認証された秘密鍵に基づいて、前記情報端末からデジタル署名を要求された電子メールに対してデジタル署名を行う署名手段を有することを特徴とする請求項1～7の何れかに記載の通信システム。

【請求項9】 情報端末に対して公開鍵暗号方式でWeb電子メールサービスを行うサーバを有する通信システムの制御方法において、

前記サーバは、前記公開鍵暗号方式における秘密鍵を管理する管理工程を有することを特徴とする通信システムの制御方法。

【請求項10】 前記管理工程は、前記秘密鍵の使用許諾を認証するための画面データを前記情報端末に供給する供給工程を含むことを特徴とする請求項9記載の通信システムの制御方法。

【請求項11】 前記管理工程は、前記供給工程により供給された前記秘密鍵の使用許諾を認証するための画面データにおいて、該秘密鍵を暗号化する際に用いられたパスフレーズが前記情報端末から入力されることを条件として該秘密鍵の使用許諾を認証する認証工程を含むことを特徴とする請求項9又は10記載の通信システムの制御方法。

【請求項12】 前記認証工程は、前記情報端末とサーバとの間において連続的に確立されている暗号通信を単位として前記秘密鍵の使用許諾を認証することを特徴とする請求項11記載の通信システムの制御方法。

【請求項13】 前記認証工程は、前記情報端末とサーバとの間に一旦確立された暗号通信が異常終了し、その後同一の情報端末との間に暗号通信が確立された場合は、該異常終了に係る暗号通信に対して認証したままの秘密鍵の使用許諾を停止する操作を行うように該情報端末に指示することを特徴とする請求項11又は12記載の通信システムの制御方法。

【請求項14】 前記認証工程は、前記情報端末とサーバとの間に暗号通信が確立されて前記秘密鍵の使用許諾を認証した後、一定時間経過することにより

認証に係る秘密鍵の使用許諾を取消すことを特徴とする請求項11～13の何れかに記載の通信システムの制御方法。

【請求項15】 前記サーバは、前記認証工程により使用許諾が認証された秘密鍵に基づいて、前記情報端末から復号処理を要求された暗号化に係るWeb電子メールを復号して、該情報端末に送信する復号工程を有することを特徴とする請求項9～14の何れかに記載の通信システムの制御方法。

【請求項16】 前記サーバは、前記認証工程により使用許諾が認証された秘密鍵に基づいて、前記情報端末からデジタル署名を要求された電子メールに対してデジタル署名を行う署名工程を有することを特徴とする請求項9～15の何れかに記載の通信システムの制御方法。

【請求項17】 情報端末に対して公開鍵暗号方式でWeb電子メールサービスを行うサーバを有する通信システムに適用可能なコンピュータ読取可能な媒体において、

前記サーバは、前記公開鍵暗号方式における秘密鍵を管理する管理ルーチンを有することを特徴とする媒体。

【請求項18】 前記管理ルーチンは、前記秘密鍵の使用許諾を認証するための画面データを前記情報端末に供給する供給ルーチンを含むことを特徴とする請求項17記載の媒体。

【請求項19】 前記管理ルーチンは、前記供給ルーチンにより供給された前記秘密鍵の使用許諾を認証するための画面データにおいて、該秘密鍵を暗号化する際に用いられたパスフレーズが前記情報端末から入力されることを条件として該秘密鍵の使用許諾を認証する認証ルーチンを含むことを特徴とする請求項17又は18記載の媒体。

【請求項20】 前記認証ルーチンは、前記情報端末とサーバとの間において連続的に確立されている暗号通信を単位として前記秘密鍵の使用許諾を認証することを特徴とする請求項19記載の媒体。

【請求項21】 前記認証ルーチンは、前記情報端末とサーバとの間に一旦確立された暗号通信が異常終了し、その後同一の情報端末との間に暗号通信が確立された場合は、該異常終了に係る暗号通信に対して認証したままの秘密鍵の使

用許諾を停止する操作を行うように該情報端末に指示することを特徴とする請求項19又は20記載の媒体。

【請求項22】 前記認証ルーチンは、前記情報端末とサーバとの間に暗号通信が確立されて前記秘密鍵の使用許諾を認証した後、一定時間経過することにより認証に係る秘密鍵の使用許諾を取消すことを特徴とする請求項19～21の何れかに記載の媒体。

【請求項23】 前記サーバは、前記認証ルーチンにより使用許諾が認証された秘密鍵に基づいて、前記情報端末から復号処理を要求された暗号化に係るWeb電子メールを復号して、該情報端末に送信する復号ルーチンを有することを特徴とする請求項17～22の何れかに記載の媒体。

【請求項24】 前記サーバは、前記認証ルーチンにより使用許諾が認証された秘密鍵に基づいて、前記情報端末からデジタル署名を要求された電子メールに対してデジタル署名を行う署名ルーチンを有することを特徴とする請求項17～23の何れかに記載の媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、Web (World Wide Web) ブラウザ上に表示可能な1つのコンテンツサービスとしての電子メール（本明細書において、Web電子メールという）サービスに関し、特にそのセキュリティ技術に関する。

【0002】

【従来の技術】

近年、情報端末とアプリケーションサーバとの間の通信においてもセキュリティを重視する傾向が強くなり、多用な用途に合わせて各種の暗号通信プロトコルが使用されている。その中でも、公開鍵暗号方式による暗号通信は、最も頻繁に使用されている。この公開鍵方式をWebコンテンツに用いる場合には、SSL (Secure Sockets Layer) と呼ばれる暗号プロトコルを使用することが多い。このWeb暗号方式においては、次世代の世界標準暗号プロトコルとして、TLS (Transport Layer Security)

というプロトコルも使用されつつある。

【0003】

さらに、電子メールにおいては、PGP (Pretty Good Privacy) やS/MIME (Secure Multipurpose Internet Mail Extensions) という方式にて暗号化することが考えられてきた。この電子メールの暗号化方式では、専用の電子メールアプリケーション（メールとも呼ばれる）を用いて公開鍵で暗号化された電子メールを、情報端末上に取得し、情報端末内に保存しておいた秘密鍵を用いて受信メールを復号化して読んだり、当該秘密鍵を用いて作成メールに署名して送信したりすることができる。

【0004】

また、最近では、モバイル情報端末の利便性を考慮した方式として、電子メールを特定端末から読むのではなく、Webブラウザを介した認証手段によって、個人のメールボックスをアプリケーションサーバ（例えばプロバイダのサーバ）上に開設することによって、専用の電子メールアプリケーションを使用せず、Webブラウザ上に表示可能な1つのコンテンツサービスとしての電子メール（Web電子メール）サービスを行うアプリケーションサーバが実現されている。もちろん、一般的に、Webブラウザアプリケーションの方が、専用電子メールアプリケーションより汎用的であるために、このようなWeb電子メールサービスが提供される要因になっている。

【0005】

【発明が解決しようとする課題】

しかし、Web電子メールサービスにおいて暗号通信を行う場合、従来のように情報端末内に秘密鍵を保存すると、当該情報端末からしか暗号化されたWeb電子メールを読むことができず、多数の情報端末からアクセスできるというWeb電子メールサービスの利便性を有効に活用することができなかった。

【0006】

本発明は、このような背景に鑑みなされたもので、その課題は、多数の情報端末から暗号化されたWeb電子メールを読めるようにすることにある。

【0007】

【課題を解決するための手段】

上記課題を解決するため、本発明は、情報端末に対して公開鍵暗号方式でWeb (World Wide Web) 電子メールサービスを行うサーバを有する通信システムにおいて、前記サーバは、前記公開鍵暗号方式における秘密鍵を管理する管理手段を有している。

【0008】

また、本発明は、情報端末に対して公開鍵暗号方式でWeb電子メールサービスを行うサーバを有する通信システムの制御方法において、前記サーバは、前記公開鍵暗号方式における秘密鍵を管理する管理工程を有している。

【0009】

また、本発明は、情報端末に対して公開鍵暗号方式でWeb電子メールサービスを行うサーバを有する通信システムに適用可能なコンピュータ読取可能な媒体において、前記サーバは、前記公開鍵暗号方式における秘密鍵を管理する管理ルーチンを有している。

【0010】

【発明の実施の形態】

以下、本発明の実施の形態を図面に基づいて説明する。

【0011】

【第1の実施形態】

図1は、本発明の第1の実施形態を適用した通信システムのシステム構成図であり、情報端末1は、中継局3、公衆網4、及びインターネット網5を介してアプリケーションサーバ2と接続されている。また、情報端末1は、PPP (Point-to-Point Protocol) 等のプロトコルにより、インターネット網5に予め接続されている。

【0012】

情報端末1は、図2に示したように、CPU51、ROM52、RAM53を具備している。また、液晶パネル、バックライト、光学系などからなる表示デバイス54を具備し、この表示デバイス54は、表示制御回路55により制御・駆

動される。これらCPU51、ROM52、RAM53、表示制御回路55は、CPUバス60を介して接続されている。

【0013】

また、CPU51は、I/Oポートを介して、通信デバイス56と通信制御回路57、及び入力デバイス58と入力制御回路59が接続されている。

【0014】

このような構成の下で、CPU51は、RAM53をワークエリア等として利用しながら、ROM52に格納されたプログラムに基づいて、電話サービス、Webブラウザサービス、Web電子メールサービス等の各種サービスに対応する各種処理を行う。

【0015】

アプリケーションサーバ2は、図3に示したように、CPU61、ROM62、RAM63、ハードディスク64、通信I/F部65を具備し、これらデバイスは、バス66により接続されている。ROM62には、ブートプログラム等が格納され、ハードディスク64には、システムプログラム(OS)、各種のアプリケーションプログラムが格納されている。

【0016】

CPU61は、ROM62のブートプログラムに基づいてハードディスク64上のシステムプログラムをRAM63に展開し、必要に応じてハードディスク64上のアプリケーションプログラムをRAM63に展開して実行することにより、Webサーバサービス、Web電子メールサービス等の各種サービスに対応する各種処理を行う。

【0017】

図1に示したように、情報端末1のROM52には、本発明に特有なプログラムとして、次のようなサービスに対応するプログラムが格納されている。このうち、Webブラウザサービス10は、ハイパーテキストマークアップ言語(HTML)で表記されたデータを、ハイパーテキスト転送プロトコル(HTTP)によって受信し、或るフォーマットにて解釈して適切に表示したり、データ送信を行うサービスである。

【0018】

表示サービス11は、各種のデータを表示デバイス54上に表示するサービスである。入力サービス12は、ペン等によってデジタイザ上の或る領域が押されたことを検知し、各種のサービスに入力情報を提供するサービスである。暗号通信サービス13は、Webブラウザサービス10等と連動し、アプリケーションサーバ2との間で暗号通信を確立するサービスである。

【0019】

また、図1に示したように、アプリケーションサーバ2のハードディスク64には、本発明に特有なプログラムとして、次のようなサービスに対応するプログラムが格納されている。

【0020】

このうち、Webサーバサービス20は、ハイパーテキスト転送プロトコル（HTTP）によって要求されるハイパーテキストマークアップ言語（HTML）で表記されたデータを、アプリケーションサーバ2内部から読出して転送する等のサービスである。暗号通信サービス21は、Webサーバサービス20等と連動し、Webブラウザサービス10との間で暗号通信を確立するサービスである。

【0021】

また、秘密鍵管理サービス22は、アプリケーションサーバ2上のWebサーバサービス20のデータ、例えばWeb電子メールサービスデータにおいて、当該電子メールデータにかけられた暗号を復号したり、或いは作成した電子メールにデジタル署名したりするために必要な公開鍵暗号に対応する秘密鍵を使用できるように管理するサービスである。

【0022】

なお、ここでは、説明の都合上、公開鍵暗号方式の公開鍵及び秘密鍵は、ユーザが使用する電子メールアドレスにより識別可能に構成されている。また、これら公開鍵と秘密鍵は、唯一無二の鍵として常に一对で存在している。

【0023】

また、Web電子メールサービス23は、Webサーバサービス20上で動作

し、電子メールアプリケーションをハイパーテキストマークアップ言語化してWebブラウザサービス10で表示できるようにすると共に、Webブラウザサービス10から電子メールの受信、作成、送信、保存等の操作を可能にするサービスである。

【0024】

なお、アプリケーションサーバ2は、上記のサービスの他に、データベース検索、リモートアクセス、ファイル管理等のサービスをも提供するように構成してもよい。

【0025】

図4は、アプリケーションサーバ2のWebサーバサービス20上のWeb電子メールサービス23に対して、情報端末1のWebブラウザサービス10でアクセスした場合の情報端末1の画面例を示す図である。

【0026】

図5は、アプリケーションサーバ2のWebサーバサービス20上のWeb電子メールサービス23に対する情報端末1のWebブラウザサービス10によるアクセスが成功し、Web電子メールの受信箱のメールを開いた場合の情報端末1の画面例を示す図である。

【0027】

図6は、アプリケーションサーバ2のWebサーバサービス20上のWeb電子メールサービス23に対する情報端末1のWebブラウザサービス10によるアクセスが成功し、復号ソフトウェアボタン押した時に、アプリケーションサーバ2から送信されて情報端末1に表示された秘密鍵使用許諾認証用の画面例を示す図である。

【0028】

図7は、アプリケーションサーバ2のWebサーバサービス20上のWeb電子メールサービス23に対する情報端末1のWebブラウザサービス10によるアクセスが成功し、復号ソフトウェアボタン押した時に、秘密鍵使用許諾認証に成功し、暗号Web電子メールが復号された場合の情報端末1の画面例を示す図である。

【0029】

図8は、アプリケーションサーバ2のWebサーバサービス20上のWeb電子メールサービス23に対する情報端末1のWebブラウザサービス10によるアクセスが成功し、秘密鍵使用許諾認証にも成功した後で、新規の電子メールを作成する場合の情報端末1の画面例を示す図である。

【0030】

図9は、図8のように新規の電子メールを作成した後、署名ソフトウェアボタンを押して、Web電子メールにデジタル署名を施した場合の情報端末1の画面例を示す図である。

【0031】

図10～11は、本発明の第1の実施形態における情報端末1の処理を示すフローチャートである。図12は、本発明の第1の実施形態におけるアプリケーションサーバ2の処理を示すフローチャートである。図13は、図12の続きのフローチャートである。図14は、情報端末機1における署名処理を示すフローチャートであり、図15は、アプリケーションサーバ2における署名処理を示すフローチャートである。

【0032】

次に、本発明に特有な処理を図10～15のフローチャートに従って詳細に説明する。

【0033】

最初に、情報端末1のWebブラウザサービス10にて、アプリケーションサーバ2上のWeb電子メールサービス23をセキュアに呼び出すためのアドレス(URL:Uniform Resource Locators、またはURI:Uniform Resource Indicators)を、入力サービス12を介して入力して送信する(図10のステップS1010)。入力サービス12の入力方法としては、例えばソフトウェアキーボード等が挙げられる。

【0034】

アプリケーションサーバ2は、情報端末1からWeb電子メールサービス23をセキュアに呼び出すメッセージを受信すると(図12のステップS1020)

、Webサーバサービス20を介して、暗号通信サービス21からの暗号Web通信確立に必要なアプリケーションサーバ認証書を情報端末1に送信し、暗号Web通信の確立を試みる（図12のステップS1030）。

【0035】

情報端末1は、アプリケーションサーバ認証書を受信すると、当該アプリケーションサーバ認証書が許容できるものであるか否かを、予め情報端末1内に保持しているユーザが信頼している認証局：CA（Certificate Authority）の署名者リスト（ルート証明書ともいう）の公開鍵を用いて、暗号通信サービス13により検査する（図10のステップS1040）。

【0036】

その結果、受信したアプリケーションサーバ認証書が当該情報端末1にとって許容できない場合は、暗号Web通信の確立を拒否する旨のメッセージをアプリケーションサーバ2に送信する（図10のステップS1050）。アプリケーションサーバ2の暗号通信サービス21は、暗号Web通信の確立を拒否する旨のメッセージを受信すると、暗号Web通信不成立を示す表示データを情報端末1に送信して（図12のステップS1060）、終了する。情報端末1のWebブラウザサービス10は、受信した暗号Web通信不成立を示す表示データを表示サービス11を介して表示して（図10のステップS1070）、終了する。

【0037】

受信したアプリケーションサーバ認証書が当該情報端末1にとって許容できる場合は、暗号Web通信の確立を容認する旨のメッセージをアプリケーションサーバ2に送信する（図10のステップS1080）。アプリケーションサーバ2の暗号通信サービス21は、暗号Web通信の確立を容認する旨のメッセージを受信すると、暗号Web通信に必要な残りの情報の交換を、情報端末1の暗号通信サービス13との間で行い、暗号Web通信を確立させると共に、当該情報端末1との暗号通信処理を専門に行うセッションプログラム（以下、セッションという）を起動し、当該セッションが当該情報端末1との暗号データ通信の処理を司るようにする。

【0038】

このセッションは、通信プログラムの構造をモデル化したOSI（Open System Interconnection）規定の7レイヤ構造のセッション層に相当する役割を担う。また、このセッションは、情報端末1との通信が正常に終了すると当然に閉じられるが、情報端末1との通信が途切れた場合にも、一定時間後に自動的に閉じる機能を有している。

【0039】

なお、本発明では、秘密鍵の使用許諾は、情報端末1とアプリケーションサーバ2との間で連続的に確立されている暗号Web通信を単位として認証され、セッションが閉じられた場合、すなわち、或る情報端末1とアプリケーションサーバ2との間で確立されていた暗号Web通信が閉じられた場合は、後述するように、秘密鍵の使用許諾の認証も同時に取り消される。

【0040】

暗号Web通信が確立した後、アプリケーションサーバ2のWebサービス20は、情報端末1が図10のステップS1010にて要求していたWeb電子メールサービス23へのアクセス画面データを、情報端末1へ送信する（図12のステップS1090）。

【0041】

情報端末1のWebブラウザサービス10は、受信した電子メールサービス23へのアクセス画面データを解析し、表示サービス11により表示させる（図10のステップS1100）。この表示内容は、例えば図4のようになる。

【0042】

ここで、情報端末1において、ユーザが入力サービス12を利用して、図4のユーザIDの入力欄100とパスワード入力欄101に、各々適切なユーザIDとパスワードを入力し、ログインソフトウェアボタン102を押した場合、Webブラウザサービス12は、当該表示データ及び入力データを、アプリケーションサーバ2のWebサービス20へ送信する（図10のステップS1110）。入力サービス12による具体的な入力方法としては、例えば、ソフトウェアキーボード等が挙げられる。

【0043】

アプリケーションサーバ2のWebサーバサービス20は、表示データ、ユーザID及びパスワード等の入力データを受信すると（図12のステップS1120）、受信したユーザIDとパスワードが、Web電子メールサービス23へアクセス可能な正当なものとしてアプリケーションサーバ2に登録されたユーザID、パスワードであるか否かを判定する（図12のステップS1130）。

【0044】

その結果、受信したユーザID、パスワードが不当なものであれば、その旨を示す不当表示画面データを情報端末1のWebブラウザサービス10に送信する（図12のステップS1140）。情報端末のWebブラウザサービス10は、不当表示画面データを受信すると（図10のステップS1150）、その不当表示画面データを解析し、表示サービス11により表示させる（図10のステップS1160）。

【0045】

情報端末1から受信したユーザID及びパスワード等の入力データが正当であると判定された場合は、アプリケーションサーバ2のWebサーバサービス20は、Web電子メールサービス23を起動し、そのWeb電子メールサービス23の表示画面データを情報端末1のWebブラウザサービス10に送信する（図12のステップS1170）。

【0046】

情報端末1のWebブラウザサービス10は、Web電子メールサービス23の表示画面データを受信すると（図10のステップS1150）、その表示画面データを解析し、表示サービス11により表示させる（図10のステップS1180）。

【0047】

ここで、通常は、暗号化されていない平文の電子メールが表示される。また、情報端末1上の電子メールの受信表題リスト等を選択する（リンクのボタンを押す）ことによって、アプリケーションサーバ2のWebサーバサービス20を介してWeb電子メールサービス23から選択した電子メールの内容を示す画面データが、情報端末1のWebブラウザサービス10に送信され（図12のステッ

PS1190)、表示サービス11により表示される(図11のステップS1190)。ここでは、情報端末1により一通の暗号化された電子メールが選択され、その暗号化された電子メールが図5に示したように、情報端末1に表示されているものとする。

【0048】

この暗号化された電子メールを復号する場合は、図5に示した復号化ソフトウェアボタン105を押す(図11のステップS1200)。この場合、表示サービス11上の復号化ソフトウェアボタン105が押下された旨がWebブラウザサービス10に通知され、Webブラウザサービス10は、復号化ソフトウェアボタン105が押下された旨の情報、及び表示データをアプリケーションサーバ2のWebサーバサービス20に送信する。

【0049】

アプリケーションサーバ2のWebサーバサービス20により、復号化ソフトウェアボタン105が押下された旨の情報、及び表示データが受信されると(図12のステップS1210)、Web電子メールサービス23は、現在のセッションにおいて秘密鍵の使用許諾がなされているか否かを、秘密鍵管理サービス22に問い合わせて確認する(図13のステップS1220)。

【0050】

その結果、現在のセッションにおいて秘密鍵の使用許諾がなされている場合、すなわち、現在のセッションが一度使用許諾がなされたセッションとして継続している場合は、図13のステップS1320に進む。なお、同一セッションであるか否かは、セッション番号等の識別子によって判断する。

【0051】

現在のセッションにおいて秘密鍵の使用許諾がなされていない場合は、秘密鍵使用許諾認証用のパスフレーズ要求画面データを、Webサーバサービス20を介して情報端末1のWebブラウザサービス10に送信する(図13のステップS1240)。

【0052】

情報端末1のWebブラウザサービス10は、秘密鍵使用許諾認証用のパスフ

レーズ要求画面データを受信すると、その画面データを解析し、表示サービス11により表示させる（図11のステップS1250、図6参照）。

【0053】

ここで、ユーザは、情報端末1の入力サービス12を用いて、情報端末1の画面上のパスフレーズ入力窓107におけるパスフレーズ入力欄108と確認入力欄109の双方にパスフレーズを入力し、OKソフトウェアボタン110を押下する（図11のステップS1260）。なお、クリアソフトウェアボタン111を押下すると、それまでパスフレーズ入力欄108及び確認入力欄109に入力した文字列がクリアされる。入力サービス12の具体的な入力方法としては、ソフトウェアキーボード等が挙げられる。

【0054】

情報端末1のWebブラウザサービス10は、入力サービス12から秘密鍵使用許諾認証用のパスフレーズ要求画面データとパスフレーズデータを受け取り、アプリケーションサーバ2のWebサーバサービス20に送信する。

【0055】

アプリケーションサーバ2のWeb電子メールサービス23は、Webサーバサービス20を介して受信した秘密鍵使用許諾認証用のパスフレーズ要求画面データとパスフレーズデータを暗号鍵管理サービス22に渡し、当該情報端末1のセッションユーザの秘密鍵のパスフレーズとの照合を依頼する（図13のステップS1280）。

【0056】

その結果、パスフレーズが不適当であれば、Web電子メールサービス23は、パスフレーズが不適当である旨のメッセージ画面データを、Webサーバサービス20を介して情報端末1に送信して（図13のステップS1290）、パスフレーズ処理を終了し、復号ソフトウェアボタン105が押下される前の状態に戻る。情報端末1のWebブラウザサービス10は、パスフレーズが不適当である旨のメッセージ画面データを受信すると（図11のステップS1300）、そのデータを解析し、表示サービス11により表示させる（図11のステップS1310）。

【0057】

パスフレーズが適当であった場合は、Web電子メールサービス23は、復号要求に係る一通の電子メールを使用許諾の取れた秘密鍵で復号化し（図13のステップS1320）、当該復号化された電子メールの表示データと、復号化ソフトウェアボタン112と署名ソフトウェアボタン113の表示形状変更データを、Webサーバサービス20を介して情報端末1のWebブラウザサービス10に送信する（図13のステップS1330）。なお、復号化ソフトウェアボタン112と署名ソフトウェアボタン113の表示形状変更データは、現在のセッションにおいて秘密鍵の使用許諾が取れていることを示すために送信されるものであり、この秘密鍵の使用許諾情報は、現在のセッションの付属情報として該セッションが閉じられるまで保存される。

【0058】

情報端末1のWebブラウザサービス10は、復号化された電子メールの表示データと、復号化ソフトウェアボタン112と署名ソフトウェアボタン113の表示形状変更データを受信すると、それらデータを解析し、表示サービス11により表示させる（図11のステップS1340、図7参照）。

【0059】

このように、秘密鍵を暗号化する際に使用したパスフレーズの入力を条件として、秘密鍵の使用許諾の認証を行うことにより、ユーザの操作を簡略化することが可能となる。

【0060】

次に、アプリケーションサーバ2のWebサーバサービス20にて、情報端末1との対話処理等を管理しているセッションがあり、当該情報端末1のユーザの秘密鍵使用許諾を保持している等の場合に、作成した電子メールに対してデジタル署名する際の処理手順を説明する。

【0061】

情報端末1が図7の状態の時に、ユーザが作成ソフトウェアボタン114を押下する（図14のステップS1400）。すると、情報端末1のWebブラウザサービス10は、入力サービス12から作成ソフトウェアボタン114の押下情

報を受信し、図7の表示データと共に、アプリケーションサーバ2のWebサービス20に送信する。

【0062】

アプリケーションサーバ2のWeb電子メールサービス23は、作成ソフトウェアボタン114の押下情報、及び図7の表示データをWebサービス20を介して受信すると（図15のステップS1410）、電子メール作成画面データ、及び作成ソフトウェアハイライトデータを、Webサービス20を介して情報端末1のWebブラウザサービス10に送信する（図15のステップS1420）。

【0063】

情報端末1のWebブラウザサービス10は、受信した電子メール作成画面データ、及び作成ソフトウェアハイライトデータを解析し、表示サービス11により表示させる（図14のステップS1430、図8参照）。

【0064】

情報端末1が図8の表示状態の場合に、ユーザは、入力サービス12を用いて電子メールの文章を文章フィールドに入力する（図14のステップS1440）。この場合の入力サービス12の入力方法は、特に規定しないが、デジタイザによるペン入力や、キーボード、音声入力等が考えられる。

【0065】

電子メールの文章を入力した後、デジタル署名を行うべく、図8の署名ソフトウェアボタン113を押下する（図14のステップS1450）。すると、情報端末1のWebブラウザサービス10は、入力サービス12から署名ソフトウェアボタン113の押下情報を受信し、図8の表示データと共に、アプリケーションサーバ2のWebサービス20に送信する。

【0066】

アプリケーションサーバ2のWeb電子メールサービス23は、署名ソフトウェアボタン113の押下情報、及び図8の表示データをWebサービス20を介して受信すると（図15のステップS1460）、自セッションが秘密鍵使用許諾を保持しているか否かを、秘密鍵管理サービス22に対して問い合わせ

る(図15のステップS1470)。

【0067】

その結果、自セッションが秘密鍵使用許諾を保持していない場合は、図13のステップS1240, S1270, S1280と同様の処理を行う(図15のステップS1480)。

【0068】

自セッションが秘密鍵使用許諾を保持している場合は、アプリケーションサーバ2のWeb電子メールサービス23は、秘密鍵管理サービス22に対して、受信・作成に係る電子メールの文書に上記使用許諾に係る秘密鍵を用いてデジタル書名を実行させ(図15のステップS1490)、そのデジタル署名がなされた電子メールの文章の表示画面データを、Webサーバサービス20を介して情報端末1のWebブラウザサービス10に送信する(図15のステップS1500)。

【0069】

情報端末1のWebブラウザサービス10は、受信したデジタル署名に係る電子メールの文章の表示画面データを解析し、表示サービス11により表示させる(図14のステップS1510、図9参照)。

【0070】

このように、公開鍵暗号方式における秘密鍵を情報端末で管理して暗号電子メールを復号することなく、アプリケーションサーバ2で管理して暗号電子メールを復号し、情報端末に送信することにより、多数の情報端末から暗号電子メールを読むことが可能となる。

【0071】

また、情報端末1から正当なパスフレーズが入力されることにより取得された秘密鍵使用許諾の情報を、アプリケーションサーバ2のセッション情報として保存することにより、暗号電子メールの復号及びデジタル署名を連続的に行うことなどが可能となると共に、当該セッションが閉じられた場合は、当該秘密鍵使用許諾も自動的に取消されることとなり、暗号電子メールの機密性を向上させることが可能となる。

【0072】

[第2の実施形態]

次に、本発明の第2の実施形態を図16～図20に基づいて説明する。

【0073】

図16は、第2の実施形態を適用した通信システムのシステム構成図であり、図1に示した第1の実施形態に係るシステム構成図と比較して、アプリケーションサーバ2にセッション管理サービス24を追加した点で相違している。

【0074】

このセッション管理サービス24は、複数の情報端末1がアプリケーションサーバ2のWebサーバサービス20にアクセスした際に、各情報端末1と個別に通信処理を行うための単位としてのセッションを管理するサービスである。

【0075】

図17、18は、第2の実施形態における情報端末1の処理を示すフローチャートである。図19、20は、第2の実施形態におけるアプリケーションサーバ2の処理を示すフローチャートであり、本フローチャートは、第1の実施形態で説明した図12のフローチャートの続きのフローだけを示している。

【0076】

以下、セッション管理サービス24が動作する場合の処理を説明する。なお、情報端末1からアプリケーションサーバ2のWeb電子メールサービス23にログオンし、暗号電子メールを表示させた後、復号ソフトウェアボタン105を押下するまでの情報端末1及びアプリケーションサーバ2の一連の動作は、第1の実施形態と同様である。

【0077】

現在のセッションについて秘密鍵の使用許諾がなされていない場合は、アプリケーションサーバ2のWeb電子メールサービス23は、セッション管理サービス24に対して、当該情報端末1が要求しているWeb電子メールの復号に用いる秘密鍵の使用許諾が、他の有効なセッションにて使用されているか否かを問い合わせる（図19のステップS2000）。

【0078】

その結果、当該情報端末1が要求しているWeb電子メールの復号に用いる秘密鍵の使用許諾が他の有効なセッションにて使用されている場合は、アプリケーションサーバ2の電子メールサービス23は、ユーザが復号ソフトウェアボタン105を再度押下するように、秘密鍵多重使用エラーメッセージを、Webサービス20を介して情報端末1のWebブラウザサービス10に送信する（図19のステップS2010）。

【0079】

情報端末1のWebブラウザサービス10は、受信した秘密鍵多重使用エラーメッセージの画面データを解析し、表示サービス11により表示させる（図17のステップS2020, S2030）。ユーザは、この秘密鍵多重使用エラーメッセージを見て、以前の異常終了時のセッションにおける秘密鍵の使用許諾が残っているものと認識し、情報端末1に表示されている復号ソフトウェアボタン105を再度押下する（図17のステップS2040）。この復号ソフトウェアボタン105の押下情報は、秘密鍵多重使用エラーメッセージの画面データと共に、Webブラウザサービス10を介してアプリケーションサーバ2のWebサービス20に送信される。

【0080】

アプリケーションサーバ2のWeb電子メールサービス23は、Webサービス20を介して復号ソフトウェアボタン105の押下情報、秘密鍵多重使用エラーメッセージの画面データを受信すると（図19のステップS2050）、秘密鍵使用停止確認メッセージの画面データを、情報端末1のWebブラウザサービス10に送信する（図19のステップS2060）。

【0081】

情報端末1のWebブラウザサービス10は、受信した秘密鍵使用停止確認メッセージの画面データを解析し、表示サービス11により表示させる（図18のステップS2070）。ここで、ユーザがOKソフトウェアボタンを押下すると（図18のステップS2080）、その押下情報は、秘密鍵使用停止確認メッセージの画面データと共に、Webブラウザサービス10を介してアプリケーションサーバ2のWebサービス20に送信される。

【0082】

アプリケーションサーバ2のWeb電子メールサービス23は、Webサーバサービス20を介してOKソフトウェアボタンの押下情報、秘密鍵使用停止確認メッセージの画面データを受信すると（図19のステップS2090）、セッション管理サービス24と秘密鍵管理サービス22へ上記情報端末1のユーザに対応する秘密鍵の使用許諾の停止を通知し（図19のステップS2100）、その応答を受けると、ステップS1240へ進み、秘密鍵使用許諾認証メッセージ画面データを、Webサーバサービス20を介して情報端末1のWebブラウザサービス10に送信する。

【0083】

図19のステップS2000にて、当該情報端末1が要求しているWeb電子メールサービスの復号に用いる秘密鍵の使用許諾が、他の有効なセッションにおいて使用されていないと判別された場合は、上記ステップS1240へ直ちに進み、秘密鍵使用許諾認証メッセージ画面データを、Webサーバサービス20を介して情報端末1のWebブラウザサービス10に送信する。

【0084】

なお、ステップS1240以降は、情報端末1、及びアプリケーションサーバ2は、第1の実施形態と同様の処理を行う。

【0085】

このように、複数のセッション（暗号通信）間で同一の秘密鍵を同時に使用する多重使用を禁止することにより、他人による秘密鍵の不正使用等を防止することが可能となる。

【0086】

なお、本発明は、上記実施形態に限定されることなく、種々変形可能である。例えば、公開鍵は、電子メールアドレスにより識別可能に構成することなく、個人を識別できるものであれば、例えば年金番号、社員番号、納税番号等により識別可能に構成してもよい。また、情報端末1のWebブラウザサービス10とアプリケーションサーバ2のWebサーバサービス20との間で授受するデータの言語は、HTMLに限定されることなく、WAP（Wireless App1

ication Protocol)、XML (Extensible Markup Language)、XHTML (the Extensible Hypertext Markup Language)、PHP (Hypertext Preprocessor) 等のマルチメディアコンテンツ記述言語を用いててもよい。

【0087】

また、秘密鍵使用認証に際し、秘密鍵を暗号化するときにかけたパスフレーズを用いて正当性を判断することなく、音声情報（声紋）、指紋、網膜（虹彩）等のバイオメトリクス情報を用いて正当性を判断してもよい。

【0088】

さらに、上記実施形態では、Web電子メールサービスをアプリケーションサーバ2が提供する前に行った暗号通信サービスとして、SSL (TLS) を用いているが、アプリケーションサーバ2と情報端末1との間で行うWeb暗号通信として、s-https、Secure-IP等の暗号通信を用いててもよい。

【0089】

また、セッションが異常終了した場合等において、使用許諾に係る秘密鍵が所定時間以上にわたって使用されないときは、自動的に当該秘密鍵の使用許諾を取り消すことも可能である。

【0090】

【発明の効果】

以上説明したように、本発明によれば、多数の情報端末から暗号化されたWeb電子メールを読むことが可能となり、利便性が向上する。

【図面の簡単な説明】

【図1】

本発明の第1の実施形態を適用した通信システムのシステム構成図である。

【図2】

情報端末の概略構成を示すブロック図である。

【図3】

アプリケーションサーバの概略構成を示すブロック図である。

【図4】

アプリケーションサーバのWeb電子メールサービスに対して、情報端末のWebブラウザサービスでアクセスした場合の情報端末の画面例を示す図である。

【図5】

Web電子メールの受信箱のメールを開いた場合の情報端末の画面例を示す図である。

【図6】

復号ソフトウェアボタン押した時に、アプリケーションサーバから送信されて情報端末に表示された秘密鍵使用許諾認証用の画面例を示す図である。

【図7】

秘密鍵使用許諾認証に成功し、暗号Web電子メールが復号された場合の情報端末の画面例を示す図である。

【図8】

秘密鍵使用許諾認証に成功した後で、新規の電子メールを作成する場合の情報端末の画面例を示す図である。

【図9】

新規の電子メールを作成した後、署名ソフトウェアボタンを押して、Web電子メールにデジタル署名を施した場合の情報端末の画面例を示す図である。

【図10】

本発明の第1の実施形態における情報端末の処理を示すフローチャートである。

【図11】

図10の続きのフローチャートである。

【図12】

本発明の第1の実施形態におけるアプリケーションサーバの処理を示すフローチャートである。

【図13】

図12の続きのフローチャートである。

【図14】

情報端末機における署名処理を示すフローチャートである。

【図15】

アプリケーションサーバにおける署名処理を示すフローチャートである。

【図16】

本発明の第2の実施形態を適用した通信システムのシステム構成図である。

【図17】

本発明の第2の実施形態における情報端末の処理を示すフローチャートである

【図18】

図17の続きのフローチャートである。

【図19】

本発明の第2の実施形態におけるアプリケーションサーバの処理を示すフローチャートである。

【図20】

図19の続きのフローチャートである。

【符号の説明】

- 1 …情報端末
- 2 …アプリケーションサーバ
- 3 …中継局
- 4 …公衆網
- 5 …インターネット網
- 10 …Webブラウザサービス
- 11 …表示サービス
- 12 …入力サービス
- 13 …暗号通信サービス
- 20 …Webサーバサービス
- 21 …暗号通信サービス
- 22 …秘密鍵管理サービス
- 23 …Web電子メールサービス

24 …セッション管理サービス

51, 61 …CPU

52, 62 …ROM

53, 63 …RAM

54 …表示デバイス

56 …通信デバイス

58 …入力デバイス

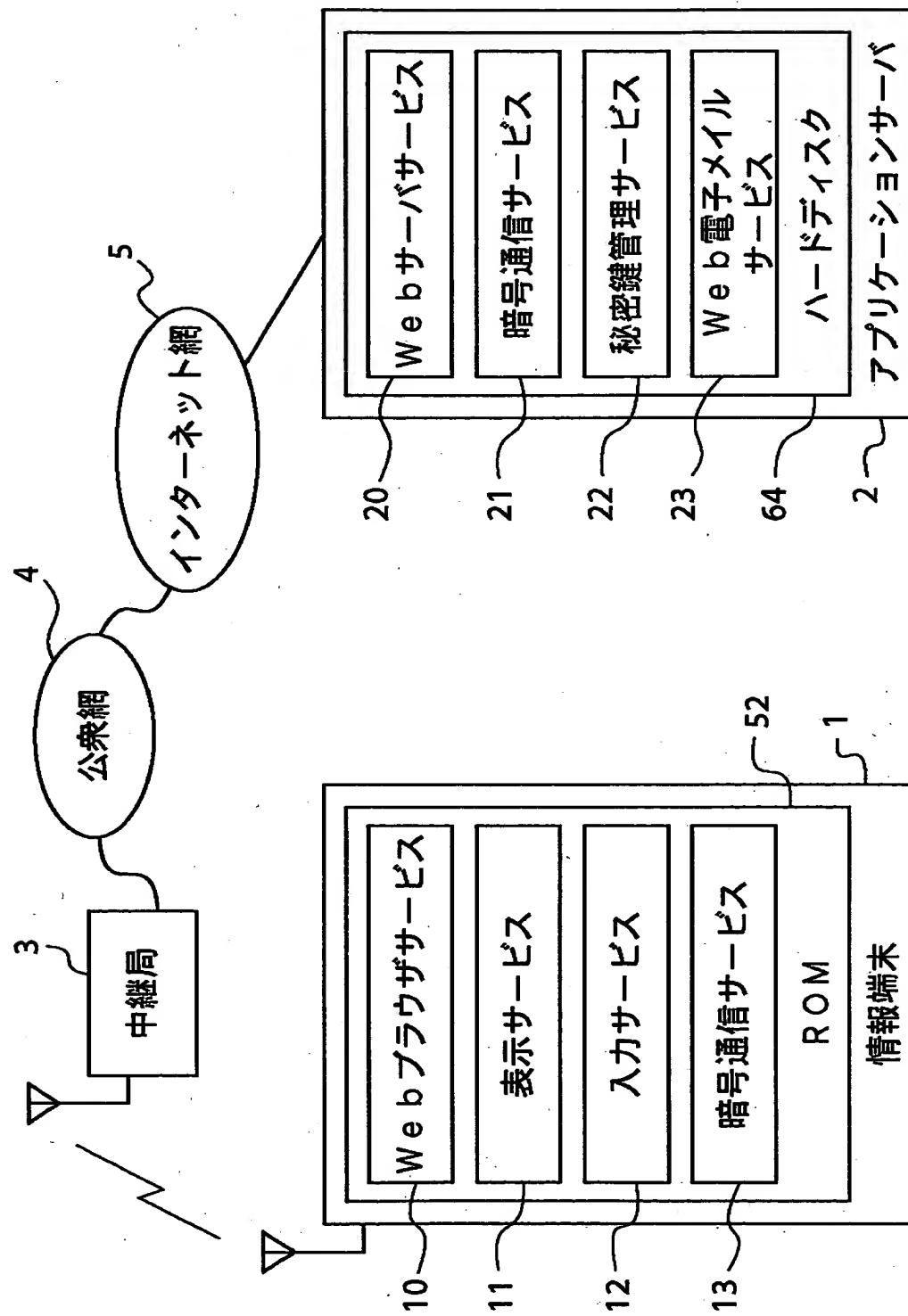
64 …ハードディスク

65 …通信I/F部

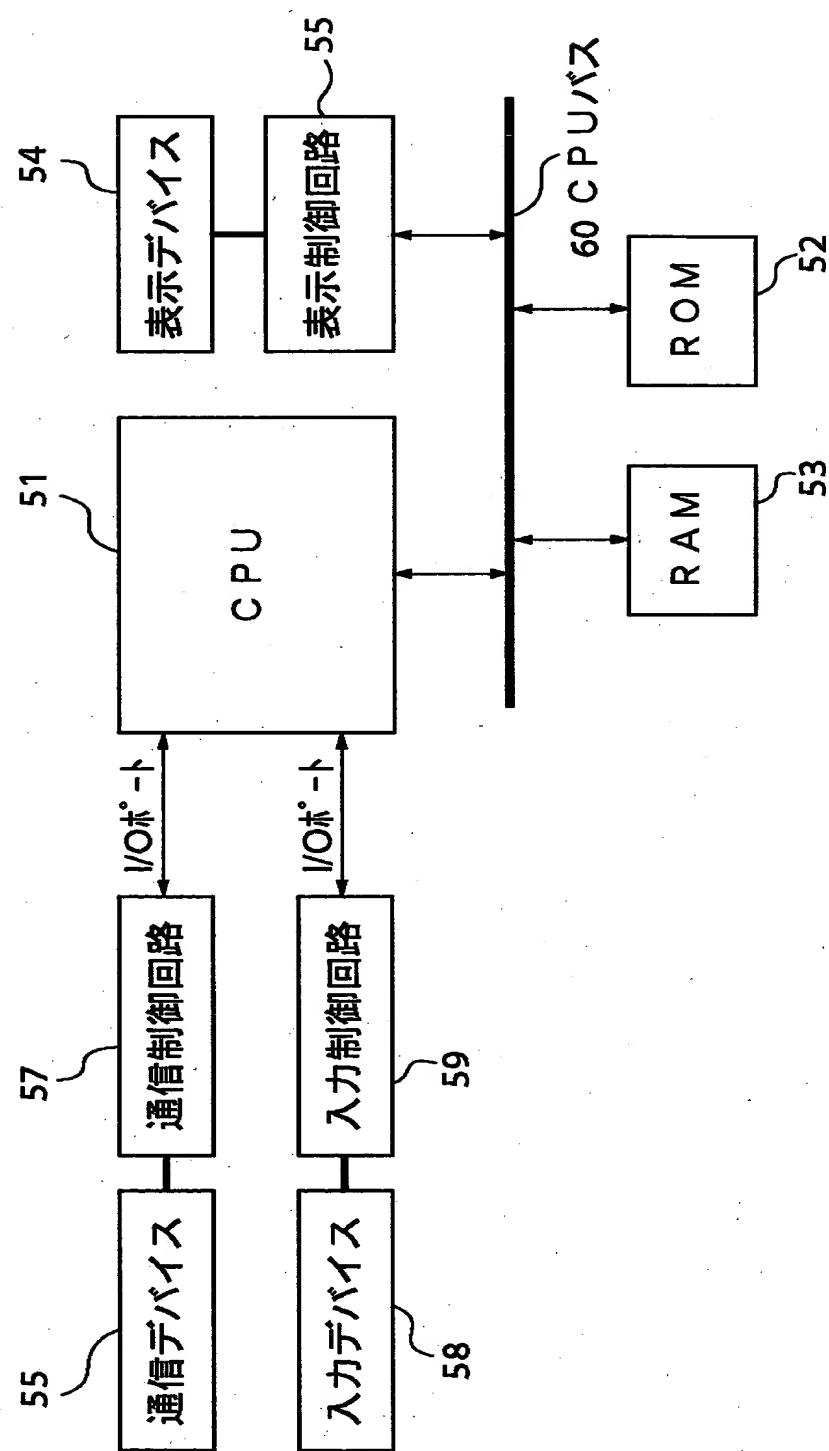
【書類名】

図面

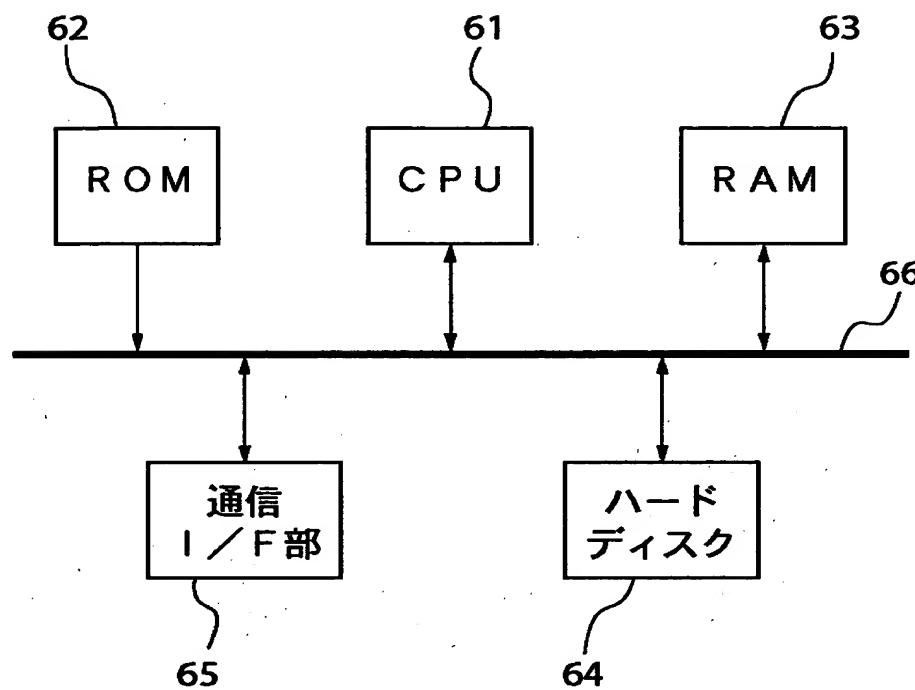
【図1】



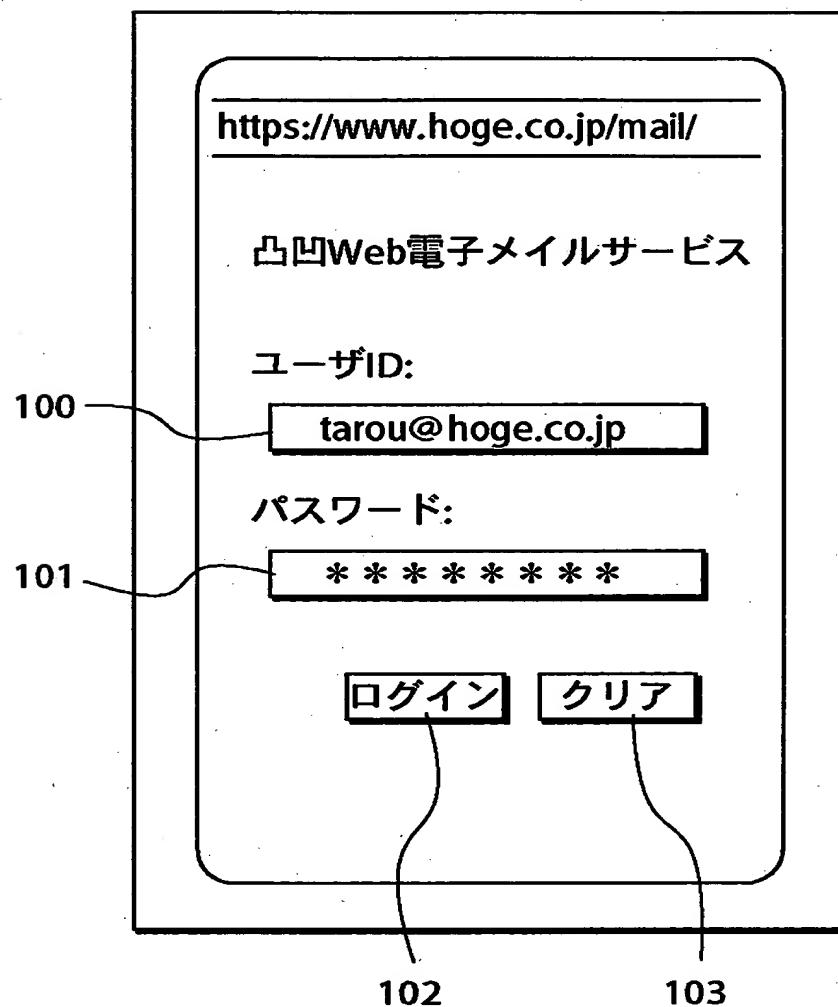
【図2】



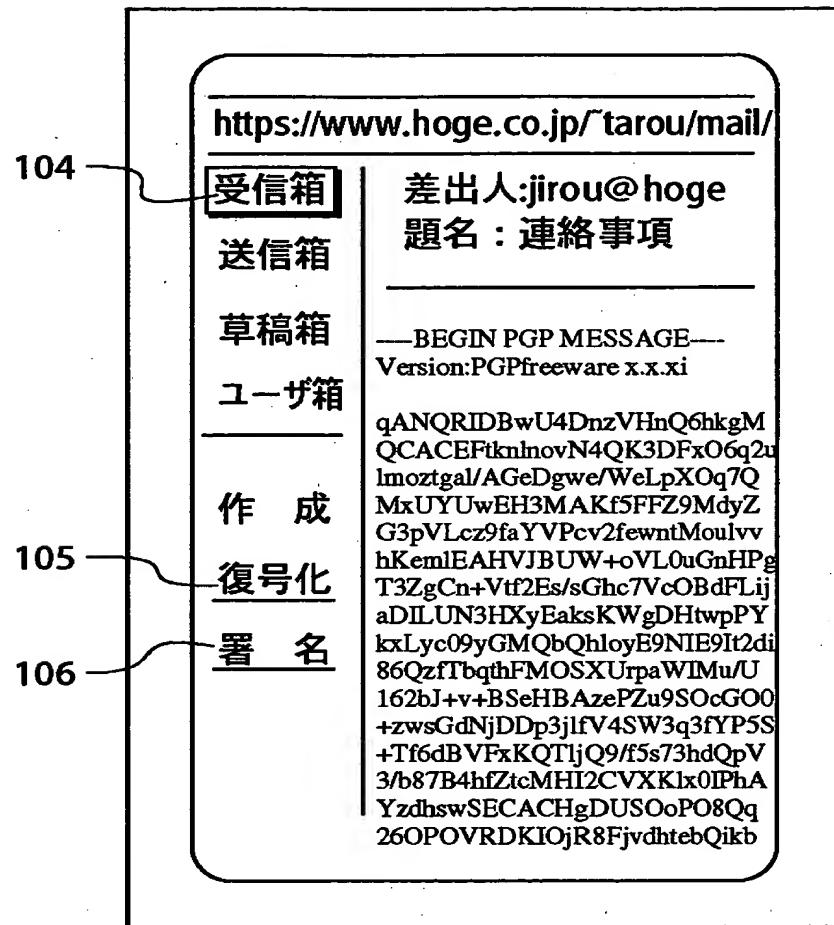
【図3】



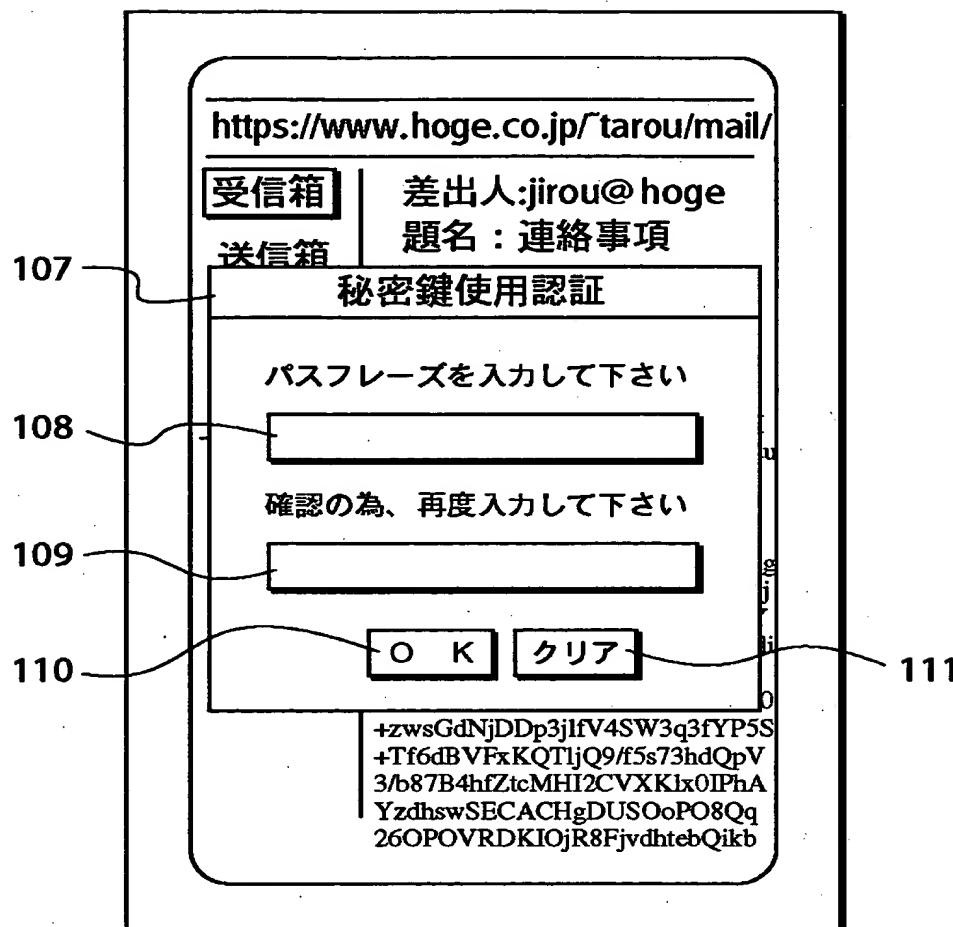
【図4】



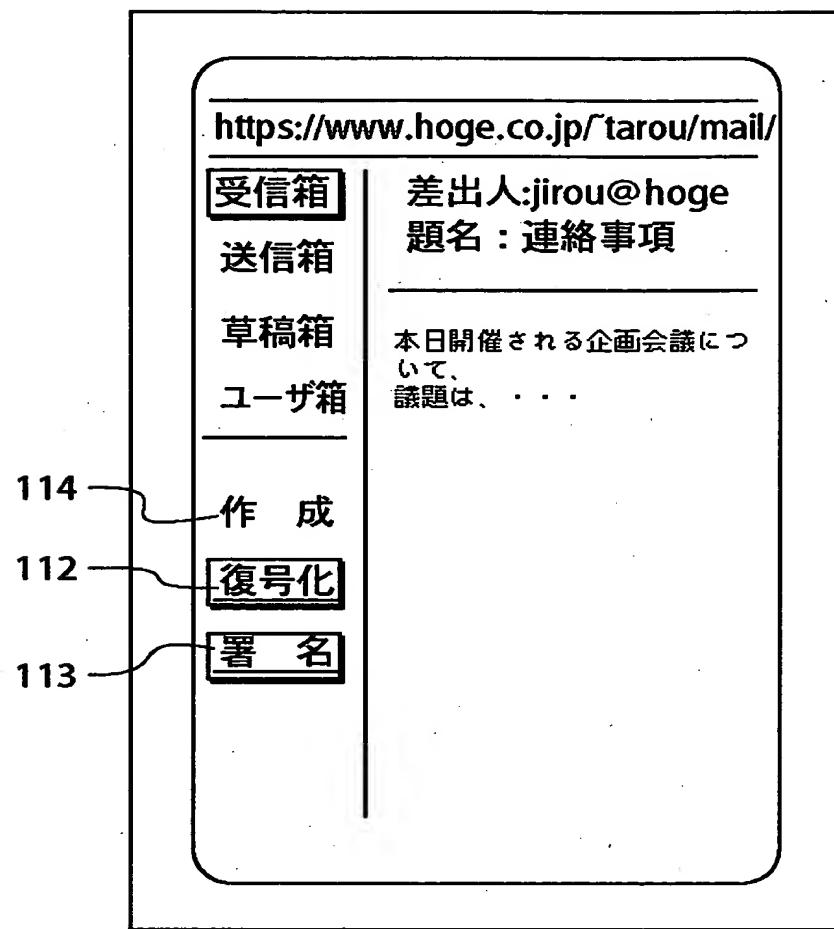
【図5】



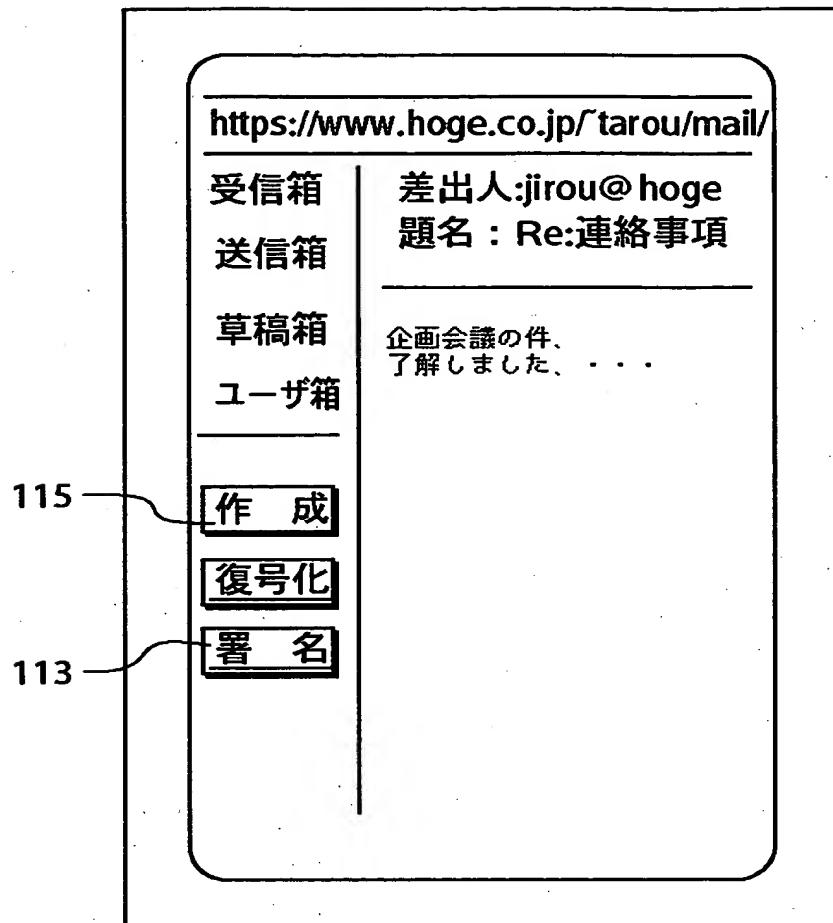
【図6】



【図7】



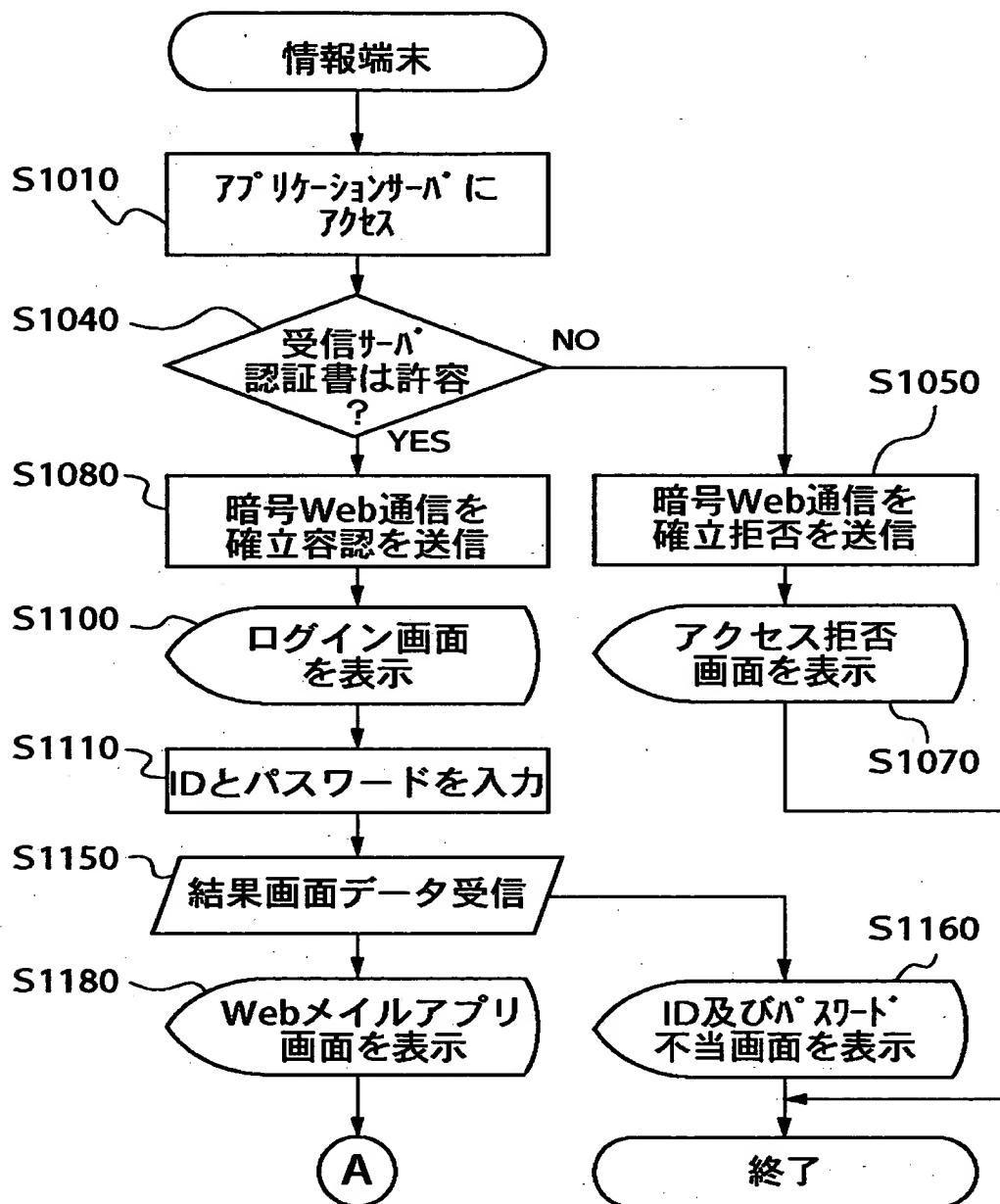
【図8】



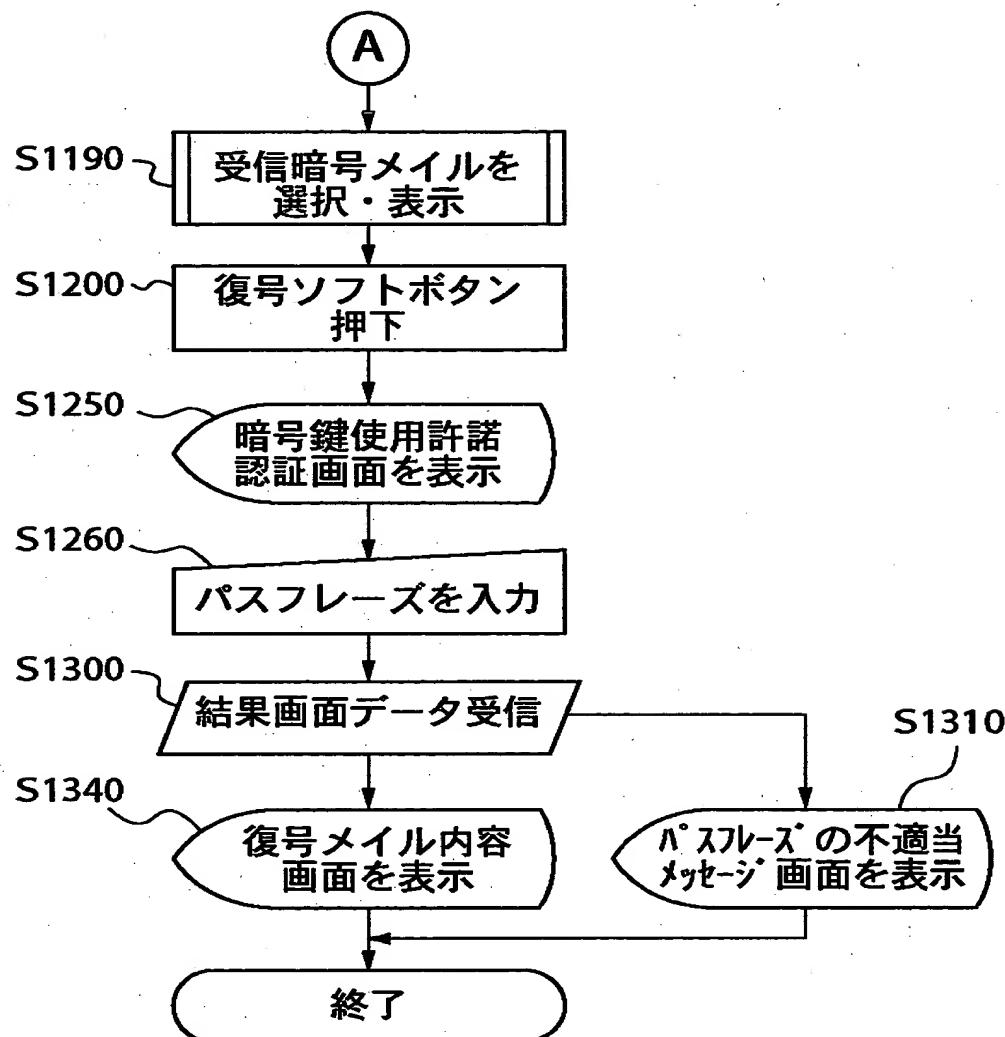
【図9】



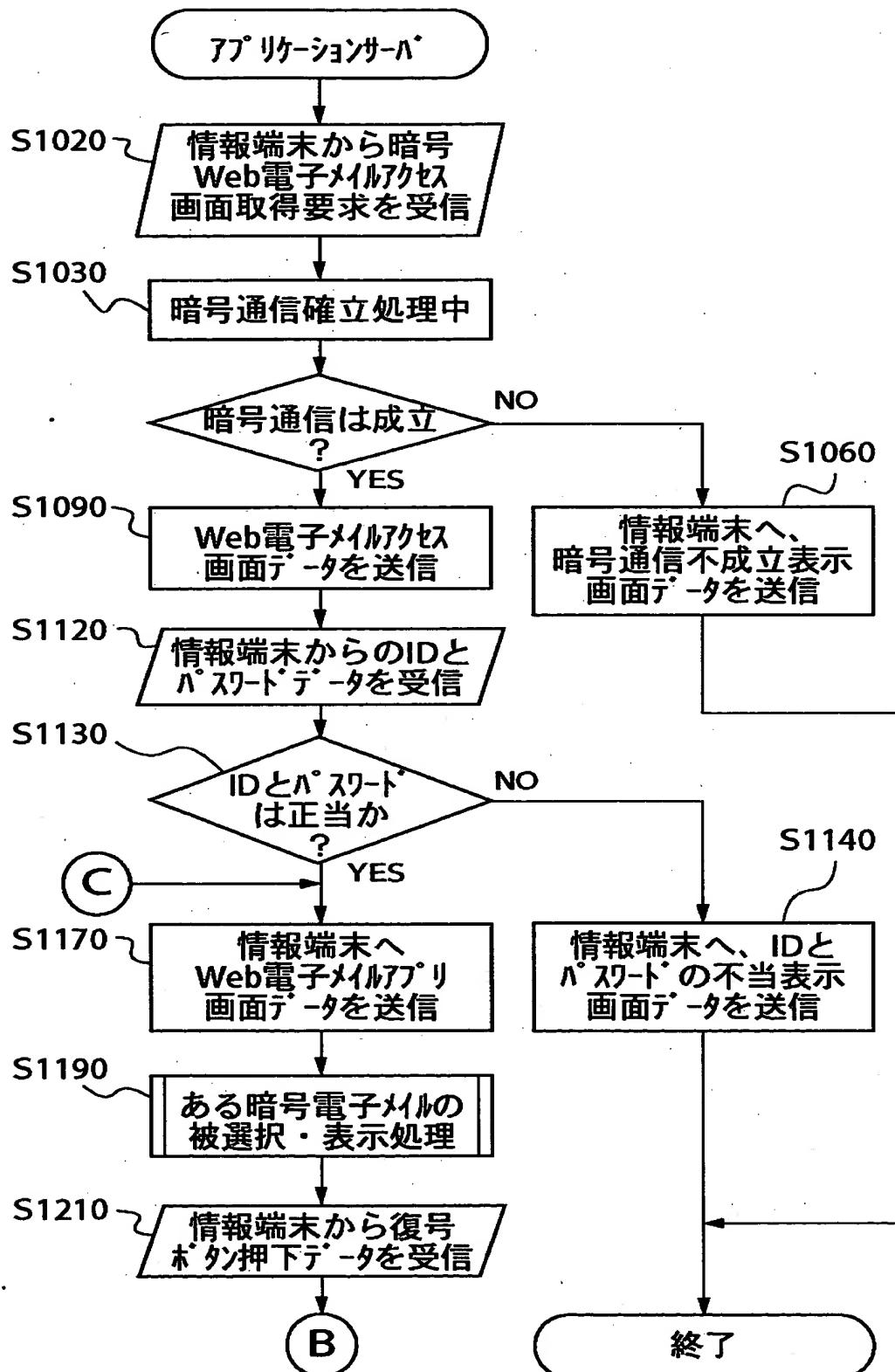
【図10】



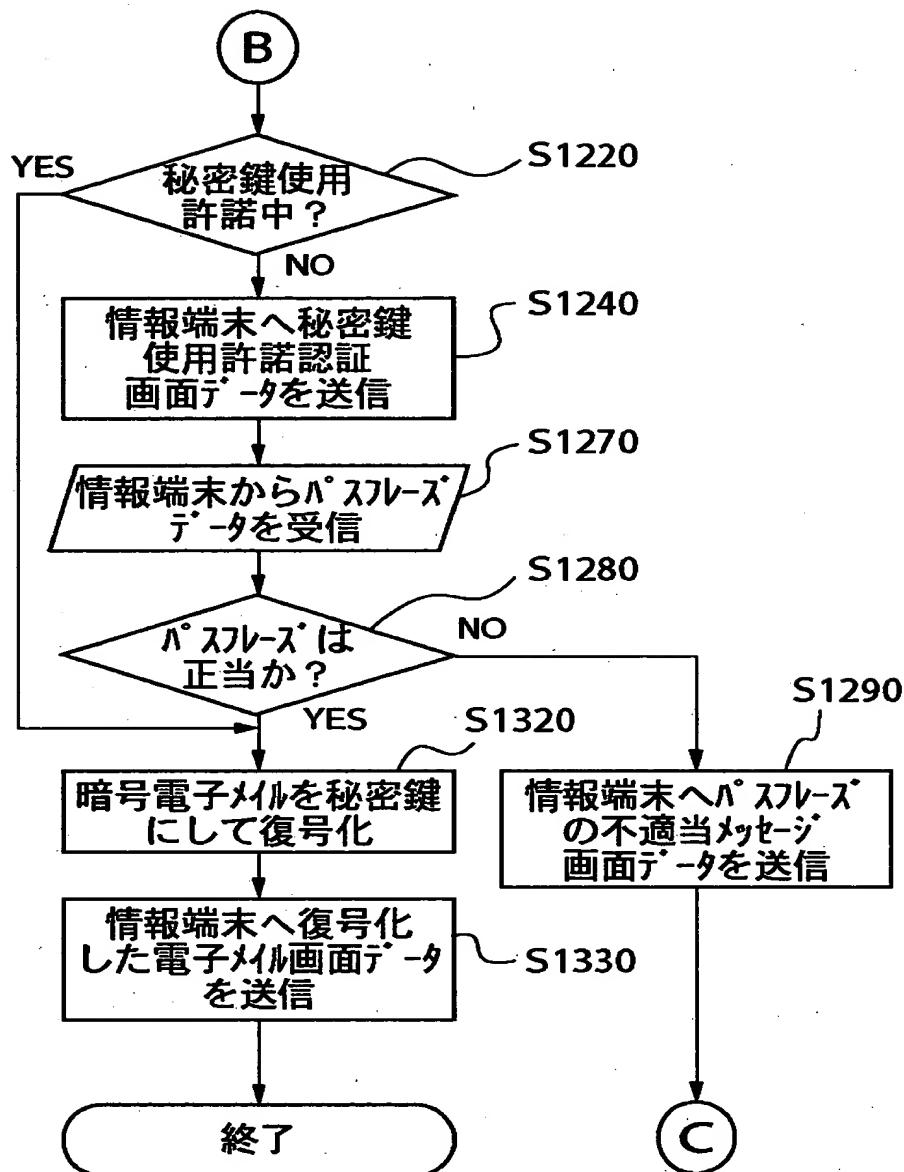
【図11】



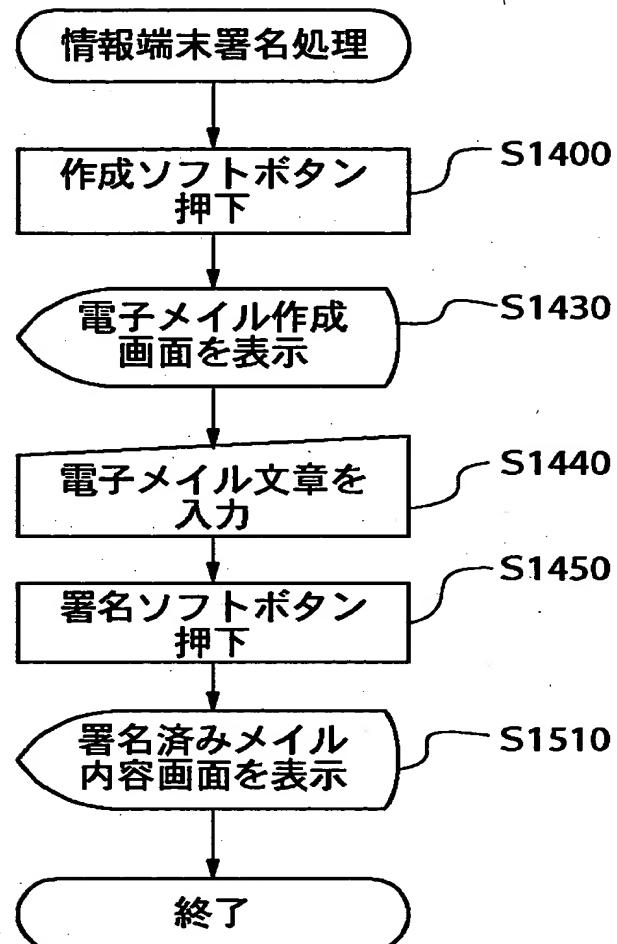
【図12】



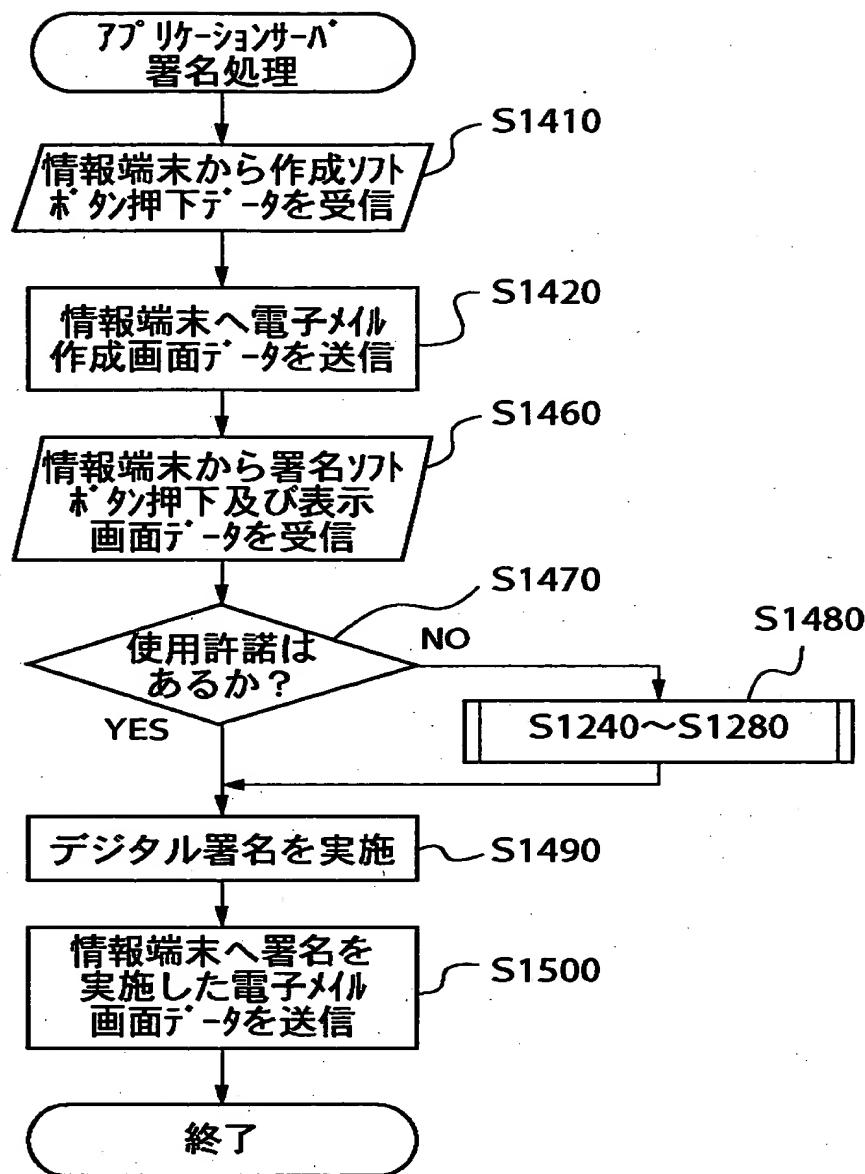
【図13】



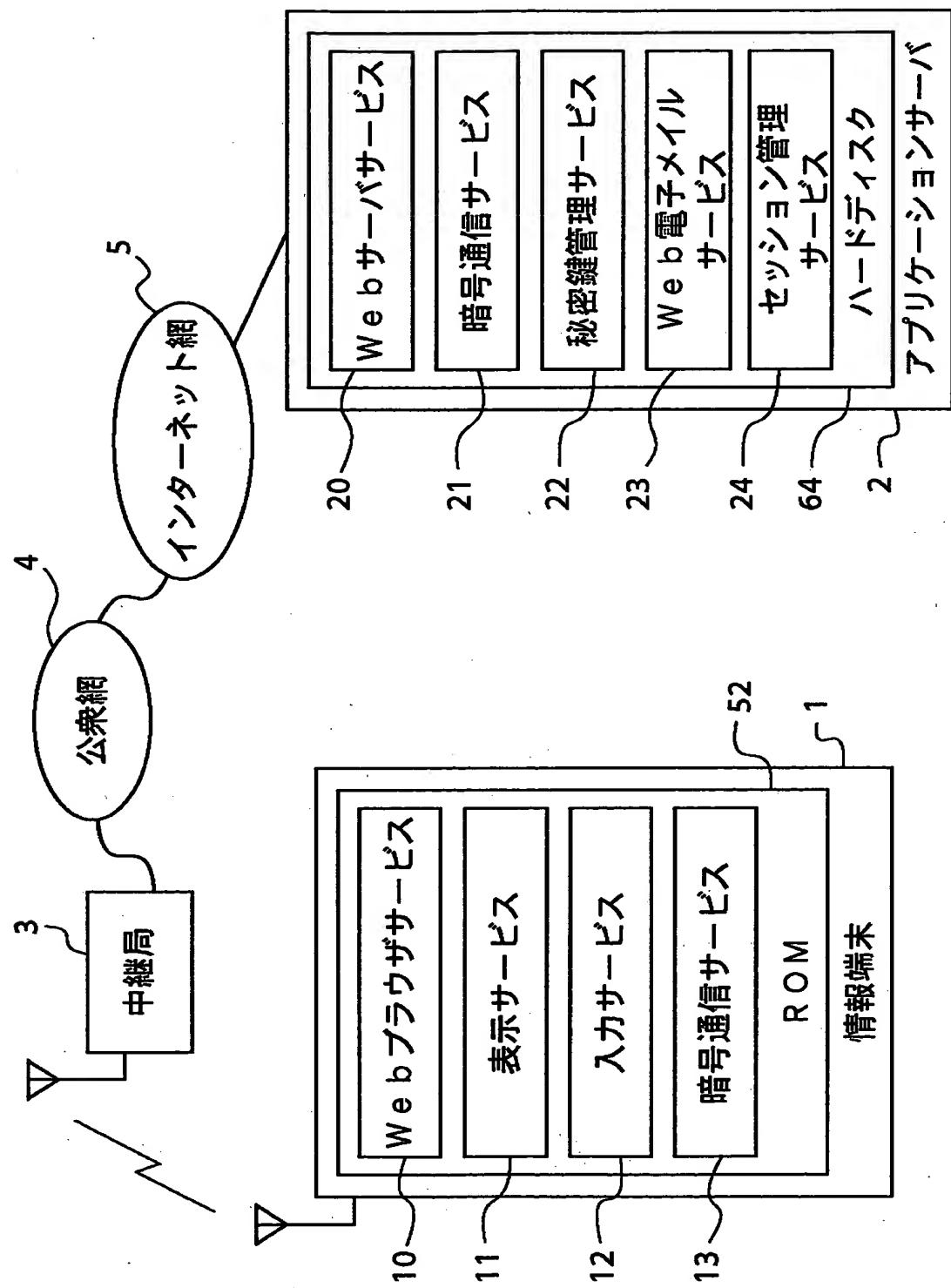
【図14】



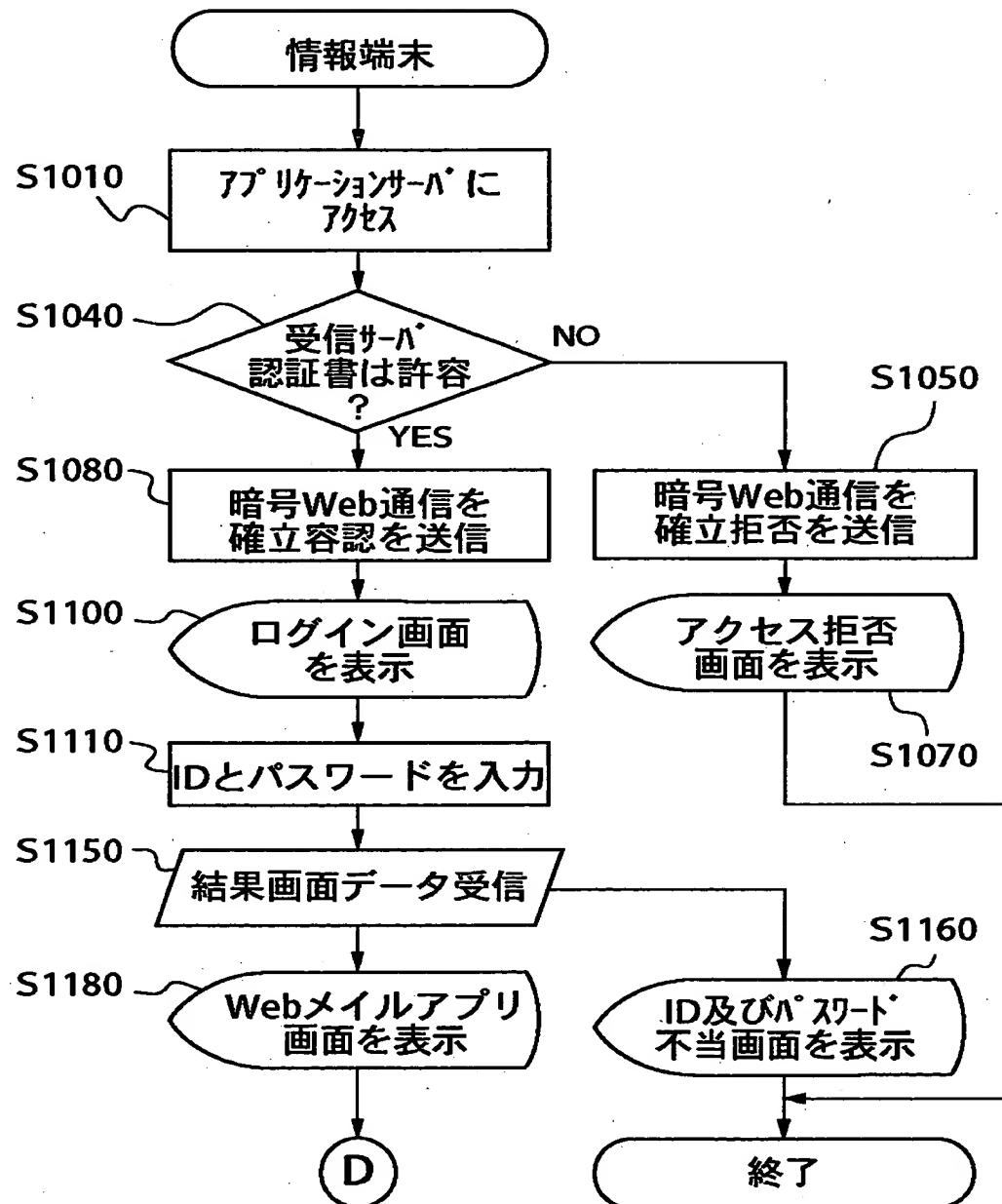
【図15】



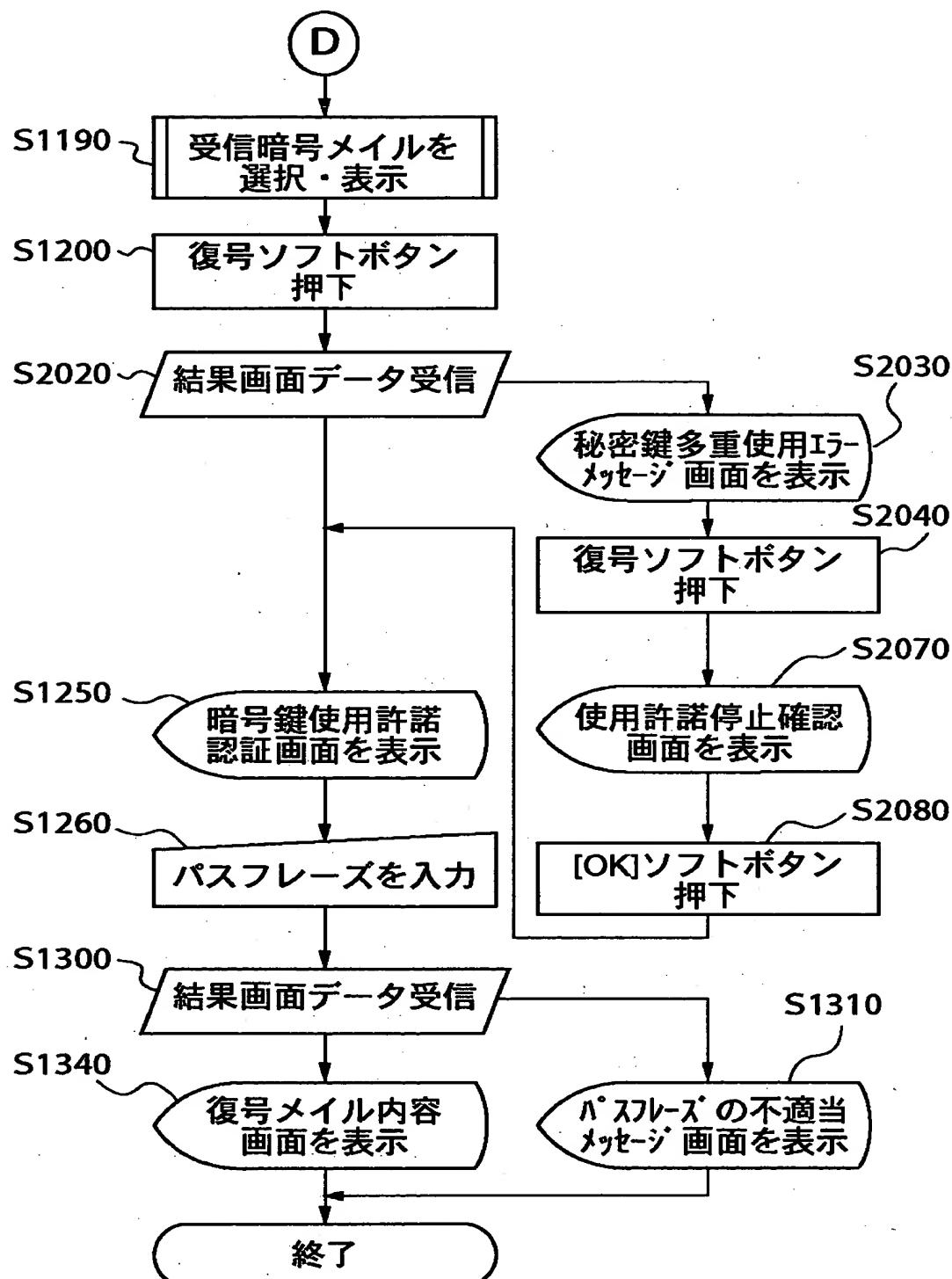
【図16】



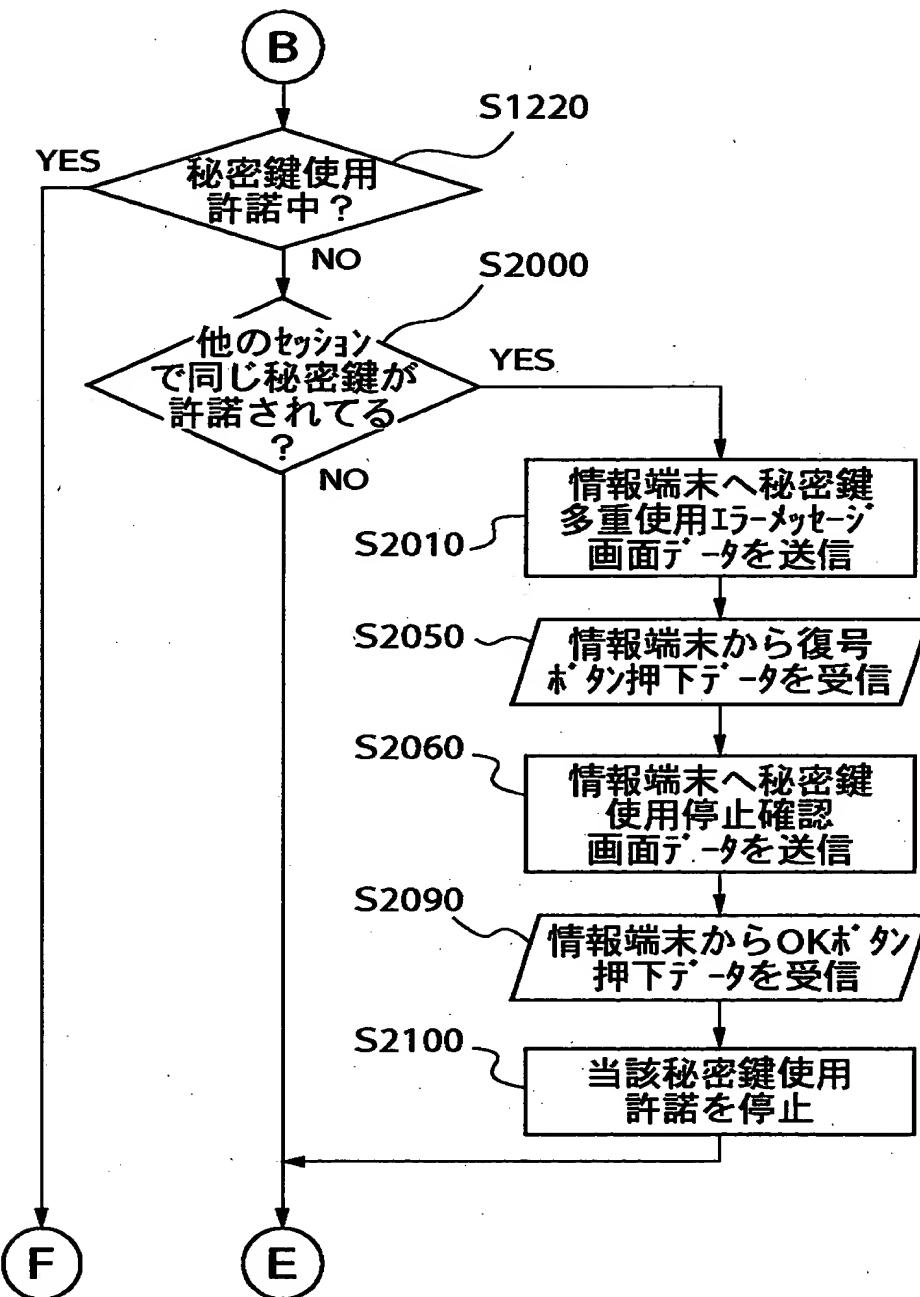
【図17】



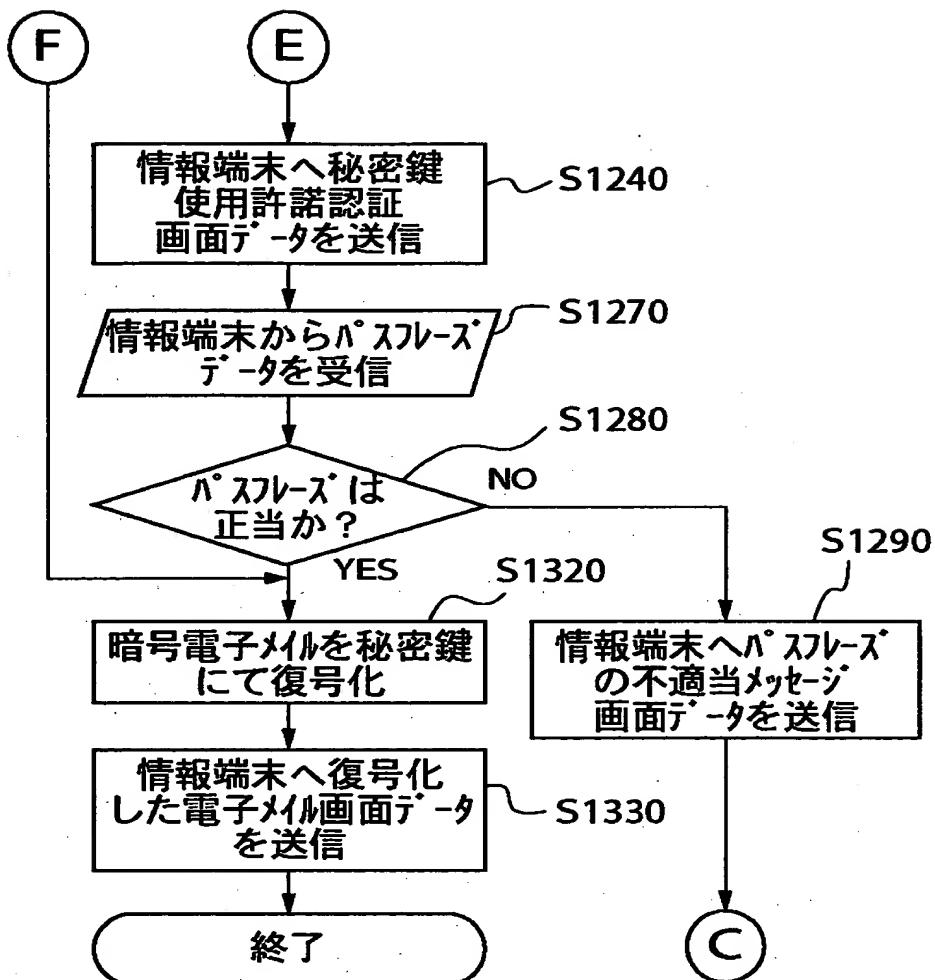
【図18】



【図19】



【図20】



【書類名】 要約書

【要約】

【課題】 多数の情報端末から暗号化されたWeb電子メールを読めるよう
にする。

【解決手段】 情報端末に対して公開鍵暗号方式でWeb（World Wide Web）電子メールサービスを行うサーバを有する通信システムにおいて、前記公開鍵暗号方式における秘密鍵を管理する管理機能、復号機能、デジタル署名機能等を前記サーバに搭載した。

【選択図】 図1

出願人履歴情報

識別番号 [000001007]

1. 変更年月日 1990年 8月30日

[変更理由] 新規登録

住 所 東京都大田区下丸子3丁目30番2号

氏 名 キヤノン株式会社